View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

JOURNAL OF ALGEBRA 29, 1–26 (1974)

The Structure of Free Irreducible, Cocommutative Hopf Algebras*

KENNETH NEWMAN

Department of Mathematics, University of Illinois at Chicago Circle, Chicago, Illinois 60680

Communicated by D. Buchsbaum

Received May 1, 1972

In [9] M. Sweedler showed that the coalgebra structure of cocommutative, irreducible Hopf algebras over perfect fields is the coproduct of "sequence of divided power" coalgebras (i.e., coalgebras whose bases consist of a sequence of divided powers). In this paper it is shown that, over perfect fields of characteristic $p > 0$ and under certain rather weak conditions, the objects in this category and in the category of commutative, cocommutative, irreducible Hopf algebras which are free over cocommutative, pointed, irreducible coalgebras are coproducts of certain elementary Hopf algebras. (B. Ditters in [2] has independently proved this theorem in some special cases.) These elementary Hopf algebras will have evident analogies to sequence of divided power coalgebras and, as shown in the appendix, are isomorphic to Witt Hopf algebras in the commutative case. The second major theorem of this paper is that if $\mathfrak{H}$ is a cocommutative, irreducible Hopf algebra and $F(\mathfrak{H})$ the free Hopf algebra of $\mathfrak{H}$, then the Hopf kernel of $F(\mathfrak{H}) \to \mathfrak{H}$ is also a coproduct of the above mentioned elementary Hopf algebras.

Section 1 consists of a listing of definitions and basic facts needed in the remainder of the paper.

Section 2 culminates in the structure theorem for free cocommutative, irreducible Hopf algebras. For this proof we need to know that these Hopf algebras contain primitives and sequences of divided powers of a certain explicit form. This is done in Propositions 2.5 and 2.10, respectively. The proof of the former strongly uses Sweedler's structure theorem, by saying in effect, for that theorem to be true, the desired primitives must exist.

Section 3 includes a demonstration that the Hopf kernel of $F(\mathfrak{H}) \to \mathfrak{H}$ is

* Part of this paper is derived from my doctoral thesis written under the direction of Professor Stephen U. Chase. I would also like to thank Professor Richard G. Larson for many useful conversations and Professor Mitsuhiro Takeuchi for pointing out some errors in the original manuscript.

Copyright © 1974 by Academic Press, Inc.
All rights of reproduction in any form reserved.

also a coproduct of these elementary Hopf algebras. This proof utilizes the methods developed in Section 2, and in addition, the relationship between Hopf algebras over fields of characteristic p and restricted Lie algebras is exploited. Included is an application of the work of E. Witt [10] on free restricted Lie algebras.

1

The following, rather long, list of definitions and results (generally previously published) is an unavoidable preliminary to the paper. Note that all diagonalization maps of coalgebras and Hopf algebras will be symbolized by Δ, and all augmentation maps by ϵ. The ground field will be denoted by $\mathfrak{K}$.

1.1. A nontrivial coalgebra will be called *simple* if it contains no nontrivial subcoalgebras.

1.2. A coalgebra is *irreducible* if it contains a unique simple subcoalgebra.

1.3. A coalgebra is *pointed* if every simple subcoalgebra is one-dimensional. Note that if $\epsilon(g) = 1$ and g is in a one-dimensional simple subcoalgebra, then g is grouplike, i.e., $\Delta g = g \otimes g$.

1.4. A Hopf algebra will be called *irreducible* if it is irreducible as a coalgebra.

Note that every irreducible Hopf algebra is pointed as a coalgebra, since the identity generates a one-dimensional subcoalgebra.

We will abbreviate pointed, irreducible, cocommutative coalgebra by PIC-coalgebra; and irreducible, cocommutative Hopf algebra by PIC-Hopf algebra. Further, the grouplike of a PIC-coalgebra will be denoted by g.

1.5. An irreducible, cocommutative bialgebra has a unique antipode, i.e., can be given a Hopf algebra structure in a unique way.

Proof. See [8, p. 71 (the first definition)] and [8, Proposition 9.2.5, p. 196].

1.6. If $\mathfrak{C}$ is a coalgebra, a sequence of subcoalgebras $\mathfrak{C}_0 \subset \mathfrak{C}_1 \subset \mathfrak{C}_2 \subset \cdots$ will be called a *filtration* if $\Delta\mathfrak{C}_i \subset \sum_{j=0}^{i} \mathfrak{C}_j \otimes \mathfrak{C}_{i-j}$ and $\bigcup_i \mathfrak{C}_i = \mathfrak{C}$.

In this paper, if $\mathfrak{C}$ is a PIC-coalgebra, we will only consider those filtrations of $\mathfrak{C}$ such that $\mathfrak{C}_0 =$ the simple subcoalgebra of $\mathfrak{C}$.

1.7. If $\mathfrak{C}$ is a PIC-coalgebra, a set of subspaces $\{\mathfrak{D}_i\}_{i=0}^{\infty}$ form a *grading* of $\mathfrak{C}$ if

(a) $\mathfrak{D}_0 =$ simple subcoalgebra of $\mathfrak{C}$;

(b) $\mathfrak{C} = \oplus_{i=0}^{\infty} \mathfrak{D}_i$;

(c) $\Delta\mathfrak{D}_i \subset \sum_{j=0}^{i} \mathfrak{D}_j \otimes \mathfrak{D}_{i-j}$.

If $\mathfrak{H}$ is a PIC-Hopf algebra then $\{\mathfrak{D}_i\}_{i=0}^{\infty}$ is a Hopf algebra grading if it is both a coalgebra and algebra grading.

1.8. If $\{\mathfrak{D}_i\}_{i=0}^{\infty}$ is a grading of $\mathfrak{C}$, then $\{\mathfrak{C}_i\}_{i=0}^{\infty}$, where $\mathfrak{C}_j = \oplus_{i=0}^{j} \mathfrak{D}_i$, will be called the *associated filtration.* (It is easy to see that it is a filtration.)

1.9. A basis $\mathfrak{B} = \{x_i\}_{i\in I}$ of a PIC-coalgebra $\mathfrak{C}$ will be called *homogeneous* with respect to a given filtration $\{\mathfrak{C}_j\}_{j=0}^{\infty}$ if

(a) for each j, there exists a subset of $\mathfrak{B}$ spanning $\mathfrak{C}_j$;

(b) $g \in \mathfrak{B}$;

(c) if $x_i \in \mathfrak{B}$ and $x_i \neq g$ then $\epsilon(x_i) = 0$.

It is clear that for any filtration there is a related homogeneous basis.

1.10. A basis $\mathfrak{B} = \{x_i\}_{i\in I}$ of a PIC-coalgebra will be *homogeneous* with respect to a given grading $\{\mathfrak{D}_i\}_{i=0}^{\infty}$ if, for each j, a subset of $\mathfrak{B}$ spans $\mathfrak{D}_j$. Note that a basis homogeneous with respect to a grading is also homogeneous with respect to the associated filtration.

1.11. Every PIC-coalgebra $\mathfrak{C}$ can be filtered, by what is called the *coradical filtration.* Let

$$\mathfrak{C}_n = \text{kernel}(\mathfrak{C} \xrightarrow{\Delta_n} \mathfrak{C}^{(n+1)} \xrightarrow{(I-\epsilon)^{(n+1)}} (\mathfrak{C}^+)^{(n+1)}),$$

where I is the identity map on $\mathfrak{C}$,

$$\mathfrak{C}^+ \equiv \{X \in \mathfrak{C} \mid \epsilon(X) = 0\}, \qquad \text{and} \qquad X^{(n)} \equiv \underbrace{X \otimes \cdots \otimes X}_{n\text{-times}}$$

(See [8, Corollary 9.0.4, p. 185 and Corollary 9.1.7, pp. 191–192].

1.12. Let $\mathfrak{C}^*$ be the algebra dual to a PIC-coalgebra $\mathfrak{C}$. Then $\mathfrak{C}$ is a $\mathfrak{C}^*$-module via $c^* \cdot c = \sum_{(c)} c_{(1)}\langle c^*, c_{(2)}\rangle$, where $c^* \in \mathfrak{C}^*$, $c \in \mathfrak{C}$, and $\Delta c = \sum_{(c)} c_{(1)} \otimes c_{(2)}$ [8, Proposition 2.11, p. 34].

1.13. Let $\mathfrak{C}$ be a PIC-coalgebra. We say a PIC-Hopf algebra $F(\mathfrak{C})$ is the free PIC-Hopf algebra on $\mathfrak{C}$ if

(a) there exists a coalgebra map $\iota : \mathfrak{C} \to F(\mathfrak{C})$

(b) for all PIC-Hopf algebras $\mathfrak{H}$ and coalgebra maps $\theta : \mathfrak{C} \to \mathfrak{H}$, there exists a unique Hopf algebra map $\psi : F(\mathfrak{C}) \to \mathfrak{H}$, such that $\iota \circ \psi = \theta$.

Remark. It is quite easy to construct free PIC-Hopf algebras. Let $\{x_i\}_{i\in I}$ be a basis for $\mathfrak{C}^+$. Then let $F(\mathfrak{C}) = \mathfrak{K}[X_i]_{i\in I}$ be the noncommutative polynomial ring on the objects $\{X_i\}_{i\in I}$. Give $F(\mathfrak{C})$ a coalgebra structure by letting the diagonalization of X_i correspond to that of x_i (with the grouplike in $\mathfrak{C}$ corresponding to the identity in $F(\mathfrak{C})$). The diagonalization of each polynomial is determined by the axiom that diagonalization is an algebra map. Finally we define $\epsilon(X_i) = 0$. Note that $F(\mathfrak{C})$ has an antipode by 1.5.

$F(\mathfrak{C})$ will be the free PIC-Hopf algebra over $\mathfrak{C}$, for

(a) The map ι generated by $x_i \to X_i$ and $g \to 1$ is a coalgebra map from $\mathfrak{C}$ to $F(\mathfrak{C})$.

(b) If $\mathfrak{H}$ is an arbitrary PIC-Hopf algebra and $\theta : \mathfrak{C} \to \mathfrak{H}$, let $\theta(x_i) = y_i$. Then define $\psi: F(\mathfrak{C}) \to \mathfrak{H}$ via $\psi(X_i) = y_i$. Clearly ψ is a Hopf algebra map.

1.14. In a similar way, we can define free PIC-Hopf algebras in the category of commutative PIC-Hopf algebras. These can be constructed by using commutative polynomial rings. If we wish to distinguish between the noncommutative and commutative free PIC-Hopf algebras of a PIC-coalgebra, the former will be denoted $nF(\mathfrak{C})$ and the latter $cF(\mathfrak{C})$. Generally, however, we will call both $F(\mathfrak{C})$.

Remark. General free Hopf algebras exist [see 7, p. 66].

1.15. If we have designated some basis $\{x_i\}_{i\in I}$ of $\mathfrak{C}^+$, then we will call $\mathfrak{K}[X_i]_{i\in I}$ (commutative or non-commutative) the canonical representation of $F(\mathfrak{C})$.

If $\{x_i\}_{i\in J\subset I}$ span $\mathfrak{D}^+$ where $\mathfrak{D}$ is a subcoalgebra of $\mathfrak{C}$ then we will denote $\mathfrak{K}[X_i]_{i\in J}$ by $F(\mathfrak{D})$.

Throughout the remainder of the paper the ground field will be a perfect field of characteristic $p > 0$.

1.16. Let $\mathfrak{B} = \{x_i\}_{i\in I}$ be a basis of $\mathfrak{C}$, a PIC-coalgebra. Define

$$v\colon \mathfrak{C}^{(p)} \equiv \underbrace{\mathfrak{C} \otimes \mathfrak{C} \otimes \cdots \otimes \mathfrak{C}}_{p\text{-times}} \to \mathfrak{C}$$

via

(a) $x_i^{(p)} \to x_i$;

(b) all other canonical basis elements of $\mathfrak{C}^{(p)} \to 0$.

Extend by $1/p$-linearity. Now define $V = \Delta_{p-1} \circ v$. Since v restricted to the symmetric tensors is independent of basis [3, Theorem 4.1.1, p. 273 and Corollary 4.1.2, p. 274], V is uniquely defined for each PIC-coalgebra.

1.17. V commutes with coalgebra and algebra maps [3, Proposition 4.1.6, p. 278–279] and, therefore, $V(\mathfrak{C})$ is a subcoalgebra of $\mathfrak{C}$ and $V(\mathfrak{H})$ is a sub-Hopf algebra of $\mathfrak{H}$.

1.18. Let

$$V^n = \underbrace{V \circ V \circ \cdots \circ V}_{n\text{-times}}.$$

We say $x \in \mathfrak{C}$ has *coheight* n if $x \in V^n(\mathfrak{C})$ and x has *coheight* ∞ if

$$x \in V^\infty(\mathfrak{C}) \equiv \bigcap_i V^i(\mathfrak{C}).$$

1.19. Let $\{\mathfrak{C}_i\}_{i=0}^\infty$ be a filtration of a PIC-coalgebra $\mathfrak{C}$. Then $V(\mathfrak{C}_n) \subset \mathfrak{C}_t$, $t =$ greatest integer $\leqslant n/p$.

Proof. Pick a homogeneous basis $\{x_i\}_{i \in I}$ of $\mathfrak{C}$. Since

$$\Delta_{p-1}(\mathfrak{C}_n) \subset \sum_{i_1+i_2+\cdots+i_p=n} \mathfrak{C}_{i_1} \otimes \mathfrak{C}_{i_2} \otimes \cdots \otimes \mathfrak{C}_{i_p}$$

and since $x_i^{(p)}$ can be in the right hand set only if $x_i \in \mathfrak{C}_t$, $V(\mathfrak{C}_n) \subset \mathfrak{C}_t$.

1.20. If $\{\mathfrak{D}_i\}_{i=0}^\infty$ is a grading of a PIC-coalgebra, then $V(\mathfrak{D}_n) \subset \mathfrak{D}_{n/p}$ if $p \mid n$ and $V(\mathfrak{D}_n) = 0$ if $p \nmid n$.

Proof. Similar to [1.19].

1.21. If $x \in \mathfrak{C}$, a PIC-coalgebra and $\epsilon(x) = 0$, then $V^m(x) = 0$ for some m.

Proof. If we take the coradical filtration of $\mathfrak{C}$ then by [1.19], $V^m(c) \in \mathfrak{C}_0$ for some m. But $\epsilon(V^m(x)) = 0$ and 0 is the only element with zero augmentation in $\mathfrak{C}_0$.

1.22. If $\mathfrak{H}$ is a PIC-Hopf algebra define

$$\mathscr{P}(\mathfrak{H}) = \{x \in \mathfrak{H} \mid \Delta x = 1 \otimes x + x \otimes 1\}.$$

Note that $\mathscr{P}(\mathfrak{H})$ is a vector space. Also if $\{\mathfrak{H}_i\}_{i=0}^\infty$ is the coradical filtration of $\mathfrak{H}$, then $\mathfrak{H}_1 = \mathfrak{H}_0 \oplus \mathscr{P}(\mathfrak{H})$ [8, Proposition 10.0.1, p. 200].

1.23. A set of elements ${}^0x, {}^1x, {}^2x,\ldots, {}^nx$ (n finite or infinite) in a PIC-Hopf algebra $\mathfrak{H}$ will be called an *n-sequence of divided powers* (n-SDP or SDP), if $\Delta^i x = \sum_{j=0}^{j} {}^jx \otimes {}^{i-j}x$. Note that ${}^0x = 1$ and ${}^1x \in \mathscr{P}(\mathfrak{H})$. At times, we will say that the above set is a SDP over ${}^1x$.

1.24. Since the $\{{}^ix\}$ in [1.23] form a graded coalgebra, [1.20] implies that $V^n(x) = {}^{n/p}x$ if $p \mid n$ and $V^n(x) = 0$ if $p \nmid n$.

1.25. Let $\| e \| \in Z_{\leqslant 0}$ be defined by $p^{\|e\|} \leqslant e < p^{\|e\|+1}$.

1.26. Let $\mathfrak{H}$ be a PIC-Hopf algebra. Assume ${}^0x, {}^1x,\ldots, {}^{t-1}x$ is a SDP such that ${}^ex$ has coheight $n - \| e \|$ for $1 \leqslant e < t$ and $t < p^{n+1}$. Then there exists a ${}^tx$ of coheight $n - \| t \|$ such that ${}^0x, {}^1x,\ldots, {}^tx$ is a SDP.

Proof. [9, Lemma 7, p. 522].

1.27. Let ${}^1x \in P(\mathfrak{H})$, $\mathfrak{H}$ a PIC-Hopf algebra.

(a) ${}^1x$ has coheight n ($n < \infty$) if and only if there exists a $p^{n+1} - 1$ SDP over ${}^1x$.

(b) Assume $V(V^\infty(\mathfrak{H})) = V^\infty(\mathfrak{H})$. Then ${}^1x$ has coheight ∞ if and only if there exists a ∞-SDP over ${}^1x$ [9, Theorem 2, p. 521] and its modification [5, Theorem 4, p. 27].

1.28. Note that the primitives of coheight n form a decreasing sequence of vector spaces as n increases. Call the vector space of primitives of coheight n (n finite or infinite), $\mathfrak{B}_n$. We will say that a PIC-Hopf algebra has a *Sweedler basis* if there exists a basis of the primitives $\{x_i\}_{i \in G_n}$ such that there exists $G_0 \supset G_1 \supset \cdots \supset G_\infty$, such that $\{x_i\}_{i \in G_n}$ is a basis of $\mathfrak{B}_n$.

1.29. A PIC-Hopf algebra $\mathfrak{H}$ will be called a GPIC-Hopf algebra if it has a Sweedler basis and $V(V^\infty(\mathfrak{H})) = V^\infty(\mathfrak{H})$.

$\mathfrak{H}$ will automatically be a GPIC-Hopf algebra if $\mathscr{P}(\mathfrak{H})$ is finite dimensional, since it is clear that $\mathfrak{H}$ has a Sweedler basis, and [5, Corollary 13, p. 33] shows $V(V^\infty(\mathfrak{H})) = V^\infty(\mathfrak{H})$.

1.30. Assume $\mathfrak{H}$ is a GPIC-Hopf algebra and let $\{{}^1x_i\}_{i \in G_0}$ be a Sweedler basis of $\mathfrak{H}$. If $i \in G_n - G_{n+1}$ (or if $i \in G_n$, if $n = \infty$), pick a $p^{n+1} - 1$ SDP ${}^0x_1, {}^1x_i, {}^2x_i,\ldots, {}^{p^{n+1}}x_i$ over x_i. If we put any arbitrary ordering on G_0, then the set of monomials of the form

$$\left\{ {}^{m_1}x_{i_1} \cdot {}^{m_2}x_{i_2} \cdots {}^{m_s}x_{i_s} \equiv \prod {}^{m_i}x_i \mid i_j < i_k \text{ if } j < k \right.$$
$$\left. \text{and } 0 \leqslant m_j \leqslant p^{n+1} - 1 \text{ if } i_j \in G_n - G_{n+1} \right\}$$

will be a basis for $\mathfrak{H}$ [9, Theorem 3, p. 521]. (Of course, we consider monomials such as ${}^{n}x_1{}^{m}x_2$ and ${}^{n}x_1{}^{m}x_2{}^{0}x_3$ to be the same, even though notationally they are different.)

Note that $\triangle(\prod {}^{m_i}x_i) = \sum(\prod {}^{n_i-j_i}x_i \otimes \prod {}^{j_i}x_i)$, where $(j_1, j_2, \ldots, j_s)$ runs from $(0, 0, \ldots, 0)$ to $(m_1, m_2, \ldots, m_s)$. When we write $\triangle(\prod {}^{m_i}x_i)$ in this form we will call it the *normal diagonalization* of $\prod {}^{m_i}x_i$. Note further, that if we partially order the $\prod {}^{i}x_i$ by saying $\prod {}^{m_i}x_i \leqslant \prod {}^{n_i}x_i$ if each $m_i \leqslant n_i$ (if x_j is not in $\prod {}^{n_i}x_i$ consider $n_j = 0$), then each tensorand in the normal diagonalization of $\prod {}^{n_i}x_i$ will be less than or equal to $\prod {}^{n_i}x_i$.

1.31. Let $\mathfrak{C}$ be a PIC-coalgebra. A *coalgebra Sweedler basis* will be a basis $\{x_i\}_{i\in G_0}$ of $\ker V$ such that there exists $G_0 \supset G_1 \supset \cdots \supset G_\infty$, such that $\{x_i\}_{i\in G_n}$ is a basis of the elements in $\ker V$ with coheight n.

1.32. A PIC-coalgebra $\mathfrak{C}$ will be called a GPIC-coalgebra if it has a coalgebra Sweedler basis and $V(V^\infty(\mathfrak{C})) = V^\infty(\mathfrak{C})$. (Using the structure theorem of 1.30 one can see that a GPIC-Hopf algebra is a GPIC-coalgebra.) As in [1.29] $\mathfrak{C}$ will automatically be a GPIC-coalgebra if $\ker V$ is finite. (The technique of [5, Corollary 13, p. 33] also applies to the case at hand.)

2

Now we begin a succession of lemmas and propositions leading to the structure theorem for free cocommutative, irreducible Hopf algebras. First we demonstrate a structure theorem for GPIC-coalgebras that bears a strong resemblance to [1.30]. In fact, in a sense, it is a generalization of [1.30] as the basis described there is regular.

DEFINITION 2.1. A set of elements $\mathfrak{S} = \{x_i\}_{i\in I}$ in a PIC-coalgebra will be called *regular* if

(1) $V(x_i) \in \mathfrak{S}$ or $V(x_i) = 0$, for all $x_i \in \mathfrak{S}$,

(2) $V(x_i) = V(x_j) \neq 0$ implies $x_i = x_j$,

(3) $\epsilon(x_i) \neq 0$ implies $x_i = g$,

(4) $0 \notin \mathfrak{S}$.

A set of nonzero elements $x_0, x_1, \ldots, x_n$ (n finite or infinite) will be called a *regular sequence* if $V(x_i) = x_{i-1}$ $1 \leqslant i \leqslant n$ and $V(x_0) = 0$.

Note that maximal regular sequences in a regular set $\mathfrak{S}$ are disjoint and that their union (together with g, if $g \in \mathfrak{S}$) equals $\mathfrak{S}$.

PROPOSITION 2.2. *Any* GPIC-*coalgebra* $\mathfrak{C}$ *has a regular basis.*

Proof. Let $\{{}_0x_i\}_{i\in G_0}$ be a Sweedler basis of $\mathfrak{C}$. If $i \in G_n - G_{n+1}$, n finite, by definition of coheight there exists a regular sequence: ${}_0x_i$, ${}_1x_i$, ..., ${}_nx_i$. If $i \in G$ then since $V(V^\infty(\mathfrak{C})) = V^\infty(\mathfrak{C})$, there exists a regular sequence in $V^\infty(\mathfrak{C})$: ${}_0x_i$, ${}_1x_i$, ${}_2x_i$, ... Let $\mathfrak{B}$ be the totality of elements $\{{}_jx_i\} \cup \{g\}$. Then we claim that $\mathfrak{B}$ is a basis (which is clearly regular) for $\mathfrak{C}$.

To show this let the span of $\mathfrak{B}$ be $\mathfrak{D}$. Assume inductively that $\ker V^t \subset \mathfrak{D}$. (Since $\{{}_0x_i\}_{i\in G_0}$ span $\ker V$, this hypothesis is true for $t = 1$.) Let $x \in \ker V^{t+1} - \ker V^t$. Since $V^t(x) \in \ker V$, we have $V^t(x) = \sum_i a_i\, {}_0x_i$, $i \in G_t$ and $a_i \in \mathfrak{K}$. Therefore, since $V^t({}_tx_i) = {}_0x_i$, $V^t(x - \sum_i a_i^{p^t}\, {}_tx_i) = 0$; which implies by induction hypothesis that $x - \sum_i a_i^{p^t}\, {}_tx_i \in \mathfrak{D}$. Therefore, $x \in \mathfrak{D}$.

Now assume that $\sum_{i,j} a_{i,j}\, {}_jx_i = 0$, $a_{i,j} \in \mathfrak{K}$ with only a finite number nonzero. Let t be the largest integer such that $a_{i,t} \neq 0$ for some i. Then

$$0 = V^t\left(\sum_{i,j} a_{i,j}\, {}_jx_i\right) = \sum_{i\in G_t} a_{i,t}^{1/p^t}\, {}_0x_i\,.$$

But the ${}_0x_i$ are independent, which means all the $a_{i,t} = 0$, i.e., the ${}_jx_i$ are independent. Q.E.D.

Remark 2.3. The monomials of [1.30] form a regular basis of $\mathfrak{H}$, as $V(\prod {}^{n_i}x_i) = \prod {}^{n_i/p}x_i$ if $p \mid n_i\ \forall i$ and is zero otherwise.

Remark 2.4. If $\mathfrak{B}$ is a regular basis of a GPIC-coalgebra $\mathfrak{C}$, then any polynomial P in the canonical representation of $F(\mathfrak{C})$ has coheight n if and only if each variable in P has coheight n.

Proof. $\Leftarrow$ Clear since V is an algebra map.

$\Rightarrow$ $\mathfrak{B}$ regular implies that the variables in $F(\mathfrak{C})$ form a regular set. Thus if M is a monomial in $F(\mathfrak{C})$, $V(M)$ is also a monomial or zero. Now assume P has coheight n, n finite. Pick $Q \in F(\mathfrak{C})$ such that $V^n(Q) = P$. Then for each monomial M in P there is a monomial M' in Q such that $V^n(M') = M$. Now the regularity of the variables implies that each variable in M has coheight n.

If coheight $P = \infty$, we have shown that each variable has coheight n for any finite n, i.e., each variable has coheight ∞. Q.E.D.

The following, seemingly innocuous, proposition is fundamental to this paper.

PROPOSITION 2.5. *Let* $\mathfrak{H}$ *be a* PIC-*Hopf algebra and* $\mathfrak{J}$ *a* GPIC-*sub-Hopf algebra. If* $x \in \mathfrak{H}$ *such that* $V(x) = 0$ *and*

$$\Delta x = x \otimes 1 + 1 \otimes x + \sum_i T_{i,1} \otimes T_{i,2}$$

with $T_{ij} \in \mathfrak{J}$, *then there exists a primitive* $\bar{x}$ *of the form* $x + w$ *with* $w \in \mathfrak{J}$.

Proof. If $x \in \mathfrak{J}$ the proof is trivial. So assume $x \notin \mathfrak{J}$. Let $\mathfrak{B} = \{{}^1z_i\}_{i\in G_0}$ be a Sweedler basis of $\mathfrak{J}$ and let $\{\prod {}^{n_i}z_i\}$ be the basis of $\mathfrak{J}$ described in [1.30].

Let $\mathfrak{J}'$ be the Hopf algebra generated by $\mathfrak{J}$ and x. Note that if $v \in \mathfrak{J}$, coheight v in $\mathfrak{J}$ equals coheight v in $\mathfrak{J}'$. (Assume $V^m(u) = v$, $u \in \mathfrak{J}'$. We can write u as a polynomial in x and elements of $\mathfrak{J}$. But any monomial that contains a power of x is in $\ker V$. Therefore, if u' is a polynomial containing only those monomials of u without powers of x, $V^m(u') = v$.) Similarly if $v \in \mathfrak{J}' - \mathfrak{J}$, coheight $v = 0$. Therefore $\mathfrak{B}$ can be extended to a Sweedler basis of $\mathfrak{J}'$ by adjoining primitives $\{{}^1y_i\}_{i\in G_0'}$ of coheight 0. Now order $G_0 \cup G_0'$ so that each element of G_0' is greater than each element of G_0. Thus, by [1.30] $\mathfrak{J}'$ has a basis of the form $\{\prod_{i\in G_0} {}^{n_i}z_i \cdot \prod_{i\in G_0'} {}^{m_i}y_i\}$. We define

$$z\left(\prod {}^{n_i}z_i \cdot \prod {}^{m_i}y_i\right) = \prod {}^{n_i}z_i$$

and

$$y\left(\prod {}^{n_i}z_i \cdot \prod {}^{m_i}y_i\right) = \prod {}^{m_i}y_i$$

and

$$|z| \cdot \left(\prod {}^{n_i}z_i \cdot \prod {}^{m_i}y_i\right) = \sum n_i$$

and

$$|y| \left(\prod {}^{n_i}z_i \cdot \prod {}^{m_i}y_i\right) = \sum m_i$$

and will abbreviate such monomials by M_i.

Write $x = \sum_j a_j M_j$, $a_j \in \mathfrak{K} - \{0\}$. We shall show first that $|z|(M_j) > 0$ implies $|y|(M_j) = 0$. Assume the contrary. Among the M_j's such that $|z|(M_j) > 0$, pick an M_n such that $|y|(M_n)$ is maximal. Define f in the dual of $\mathfrak{J}'$, by $f(y(M_n)) = 1$ and f on other basis elements equals zero. Then using the module structure defined in [1.12], and the normal diagonalization of M_j, we have

$$f \cdot \sum a_j M_j = \sum_j a_j \left(\sum_k M_{j,k'}\langle f, M_{j,k}\rangle\right)$$

where $\Delta M_j = \sum_k M_{j,k} \otimes M_{j,k'}$. Note that $|y|(M_{j,k}) \leqslant |y|(M_j)$. Thus, by the maximality of $|y|(M_n)$ for any j, there can exist a k such that $\langle f, M_{j,k}\rangle \neq 0$ only if M_j is of the form $z(M_j)\,y(M_n)$ or $|z|(M_j) = 0$. In the first case note that $f \cdot M_j = z(M_j)$ which is a basis element in $\mathfrak{J}$ and f applied to distinct M_j's of this form yields distinct basis elements. Thus,

$$f \cdot \sum a_j M_j = \sum_{j|y(M_j)=y(M_n)} a_j z(M_j) + \sum_{j|z|(M_j)=0} a_j f_j \cdot M_j .$$

Note in the second sum $|\ z\ |(f \cdot M_j) = 0$. On the other hand, $f \cdot x = x\langle f, 1\rangle + 1\langle f, x\rangle + \sum_i T_{i,1}\langle f, T_{i,2}\rangle = 1\langle f, x\rangle$ since $\langle f, \mathfrak{J}\rangle = 0$. This is a contradiction since $z(M_n) \neq 1$.

Now we will show that $|\ y\ |(M_j) = 0$ or $1\ \forall j$. Assume the contrary and pick $M_n = \prod_{i=1}^{m} {}^{n_i}y_i$ with maximal y-value. (Of course, $z(M_n) = 0$.) Let $M_n' = {}^{n_1-1}y_1 \prod_{i=2}^{m} {}^{n_i}y_i$ be a monomial similar to M_n except that one of the nonzero n_i has been lowered by one. Define f in the dual of $\mathfrak{J}'$ by $f(M_n') = 1$ and f on the other monomials is zero. Now if $f \cdot M_j \neq 0$, M_j must be of the form

$$({}^{n_1-1}y_1)\left(\prod_{i=2}^{t-1} {}^{n_i}y_i\right)({}^{n_t+1}y_t)\left(\prod_{i=t+1}^{m} {}^{n_i}y_i\right)$$

or equal to M_n'. ($|\ y\ |(M_j) \leqslant |\ y\ |(M_n') + 1$ and if $f \cdot M_j \neq 0$, $M_n' \leqslant M_j$, using the partial order mentioned in [1.30].) In the first case $f \cdot M_j = y_t$ and if $M_j = M_n'$, $f \cdot M_j = 1$. Thus, $f \cdot \sum a_i M_i = \sum a_i u_i$, where $u_i = y_t$ for some t or $u_i = 1$ or 0. In any case, the nonzero u_i's are independent and at least one is a primitive, since $f \cdot M_n = y_1$. On the other hand,

$$f \cdot x = x\langle f, 1\rangle + 1\langle f, x\rangle + \sum_i T_{i,1}\langle f, T_{i,2}\rangle = 1\langle f, x\rangle$$

since $\langle f, \mathfrak{J}\rangle = 0$. Then we again have a contradiction.

We conclude, therefore, that either $y(M_j) = 0$, or $y(M_j) = 1$ and $z(M_j) = 0$. The latter says M_j is a primitive. Consequently, x is a linear combination of elements in $\mathfrak{J}$ and primitives, which is the statement of the proposition.

DEFINITION 2.6. Let $\mathfrak{P}_n = \mathfrak{R}[Y_0, Y_1, \ldots, Y_n]$ ($n = 0, 1, \ldots, \infty$) be either a commutative or noncommutative polynomial ring. We give $\mathfrak{P}_n$ a Hopf algebra structure by first giving each variable augmentation zero. Then let $\Delta Y_0 = 1 \otimes Y_0 + Y_0 \otimes 1$. By [1.26] we can extend this to a $p - 1$ SDP in $\mathfrak{R}[Y_0]$: $1, Y_0 = {}^1y_1, {}^2y_1, \ldots, {}^{p-1}y$. Now formally define ΔY_1 so that it is a pth divided power in this sequence. Since $V(Y_1) = Y_0$ and since the image of V is a Hopf algebra, $1, {}^1y_1, {}^2y_1, \ldots, {}^{p-1}y$ all have coheight 1 in $\mathfrak{R}[Y_0, Y_1]$. Therefore using [1.26] again $1, {}^1y_1, {}^2y_1, \ldots, {}^py = Y_1$ can be extended to a $p^2 - 1$ SDP in $\mathfrak{R}[Y_0, Y_1]$. Now formally let ΔY_2 be a p^2 divided power and continue this process up to Y_n.

For convenience, we will assume that $\mathfrak{P}_n$ is graded as a bialgebra. We can do this if we assume Y_0 has grading one, and when choosing ${}^2y, {}^3y, \ldots, {}^{p-1}y$ picking only elements homogeneous of degree $2, 3, \ldots, p - 1$ respectively. Then give Y_1 grading p, and again choose ${}^ny$ $p < n < p^2$ to be homogeneous of degree n. Give Y_2 grading p^2 and continue.

Remark 2.7. (a) $\mathfrak{P}_n$ is a cocommutative, irreducible bialgebra and thus is a Hopf algebra [1.5].

(b) $\mathfrak{P}_n \subset \mathfrak{P}_{n+j}$ $j \geqslant 0$.

(c) If $\mathfrak{P}_n' = \mathfrak{K}[Y_0', Y_1', \ldots, Y_n']$ is constructed in a manner similar to $\mathfrak{P}_n$, then there exists φ: $\mathfrak{P}_n \xrightarrow{\sim} \mathfrak{P}_n'$.

Proof. Map $Y_0 \to Y_0'$. Let ${}^n y' = \varphi({}^n y)$ $1 \leqslant n < p$. Since the ${}^n y'$ are all homogeneous and in $\mathfrak{K}[Y_0']$, we can pick a homogeneous element of degree p in $\mathfrak{K}[Y_0', Y_1']$ which extends the SDP $Y_0', {}^2y', \ldots, {}^{p-1}y'$. Coheight considerations insure that this element is of the form $Y_1' + Q_1$ with $Q_1 \in \mathfrak{K}[Y_0']$. Map $Y_1 \to Y_1' + Q_1$ and let ${}^n y' = \varphi({}^n y)$ $p \leqslant n < p^2$. Again we can extend this sequence by a homogeneous element of the form $Y_2' + Q_2$ with $Q_2 \in \mathfrak{K}[Y_0', Y_1']$. Continue this process, and we obtain a graded Hopf algebra map, with $\varphi(Y_i) = Y_i' + Q_i$, $Q_i \in \mathfrak{K}[Y_0', Y_1', \ldots, Y_{i-1}']$. The map can be seen to be onto by a simple induction and is one-to-one since the $Y_i' + Q_i$ are algebraically independent.

(d) In the commutative case, $\mathfrak{P}_n$ is isomorphic to the well known Witt Hopf algebras. (See appendix.)

DEFINITION 2.8. A $p^{n+1} - 1$ SDP $1, {}^1x, {}^2x, \ldots, {}^{p^{n+1}-1}x$ (n finite or infinite) in a PIC-Hopf algebra $\mathfrak{H}$ will be called a *standard sequence* if there exists a Hopf algebra injection φ: $\mathfrak{P}_n \to \mathfrak{H}$ such that $\varphi(Y_i) = {}^{p^i}x$. ${}^{p^i}x$ will be called the ith *generator* of the standard sequence.

Remark 2.9. In a standard sequence the generators are algebraically independent.

PROPOSITION 2.10. *Let $\mathfrak{H}$ be a* PIC-*Hopf algebra which as an algebra is a commutative or noncommutative polynomial ring $\mathfrak{K}[X_i]_{i \in I}$ where the $\{X_i\}_{i \in I}$ is a regular set in $\mathfrak{H}$. Let $y_0, y_1, \ldots, y_n$ be a regular sequence in $\mathfrak{H}$ and let $\mathfrak{J}$ be any* GPIC-*subHopf algebra of $\mathfrak{H}$ such that $\Delta y_n = 1 \otimes y_n + y_n \otimes 1 + T$ with $T \in \mathfrak{J} \otimes \mathfrak{J}$. Assume there exists another sequence of elements $\bar{y}_0, \bar{y}_1, \ldots, \bar{y}_{n-1}$ such that*

(1) $\bar{y}_i = y_i + z_i$ *with* $z_i \in V(\mathfrak{J})$ $0 \leqslant i \leqslant n - 1$.

(2) *The $\bar{y}_i$'s are generators of a standard sequence.*

Then there exists $\bar{y}_n$ of the form $y_n + z_n$ such that

(1) $z_n \in \mathfrak{J}$.

(2) $\bar{y}_n$ *is an* nth*-generator of the above standard sequence.*

Proof. Let $\mathfrak{J}'$ be the Hopf algebra generated by $\mathfrak{J}$ and y_n. Since $\bar{y}_{n-1} \in V(\mathfrak{J}')$ and $V^t(\bar{y}_{n-1}) = \bar{y}_{n-1-t}$, $t \leqslant n - 1$, $\bar{y}_i$ has coheight $n - i$ in $\mathfrak{J}'$. Now, the rth term in the standard sequence ($r < p^n$) is in the algebra

generated by $y_0, y_1, \ldots, y_{\|r\|}$, which means it has coheight $n - \| r \|$. Therefore, by [1.26], the standard sequence can be extended by an $x \in \mathfrak{J}'$.

Note that $\Delta y_n = y_n \otimes 1 + 1 \otimes y_n + T$, $T \in \mathfrak{J} \otimes \mathfrak{J}$ implies (by the definition of V) that $V(y_n) \in \mathfrak{J}$. Thus $\bar{y}_{n-1} \in \mathfrak{J}$ and the first $p^{n+1} - 1$ terms in our standard sequence are in $\mathfrak{J}$. Consequently $\Delta x = x \otimes 1 + 1 \otimes x + T'$ with $T' \in \mathfrak{J} \otimes \mathfrak{J}$.

Now since $z_{n-1} \in V(\mathfrak{J})$ we can pick $w \in \mathfrak{J}$ such that $V(w) = z_{n-1}$. Then $V(x - w - y_n) = 0$ and

$$\Delta(x - w - y_n) = 1 \otimes (x - w - y_n) + (x - w - y_n) \otimes 1 + T''$$

with $T'' \in \mathfrak{J} \otimes \mathfrak{J}$. So by Proposition 2.5 there exists a primitive of the form $x - w - y_n - v$ with $v \in \mathfrak{J}$. The element $x - (x - w - y_n - v)$ will be the $\bar{y}_n$ described in the statement of the proposition with $z_n = w + v$.

To show that $\bar{y}_n$ not only extends the standard sequence but is an nth generator, we must show that the $\bar{y}_0, \bar{y}_1, \ldots, \bar{y}_n$ are algebraically independent (so that the map $\mathfrak{P}_n \to \mathfrak{H}$ will be injective). Assume inductively that $\bar{y}_0, \bar{y}_1, \ldots, \bar{y}_{n-1}$ are algebraically independent and assume that there exist nontrivial polynomials in $(n + 1)$-variables that are zero on $\bar{y}_0, \bar{y}_1, \ldots, \bar{y}_n$. Let P be one of these polynomials of smallest degree.

In the commutative case, if $\bar{y}_0$ appears in each monomial of P, factor it out, and we have a polynomial of smaller degree $= 0$. Contradiction. If $\bar{y}_0$ is not in each monomial, apply the V map and our inductive assumption yields a contradiction since $V(\bar{y}_i) = \bar{y}_{i-1}$ if $i \geqslant 0$.

In the noncommutative case, note that the first variable of at least one of the monomials in $\bar{y}_i$ differs from the first variable of all the monomials in $\bar{y}_0, \bar{y}_1, \ldots, \bar{y}_{i-1}$. For, if we pick n_j so that all the first variables in $\bar{y}_j$ are in $\ker V^{n_j}$ but not in $\ker V^{n_j-1}$, the regularity of the variables and the fact that $V(\bar{y}_j) = \bar{y}_{j-1}$ if $j \geqslant 1$ clearly implies that $n_j > n_{j'}$ if $j > j'$. Now write P in the form $\bar{y}_0 P_0 + \bar{y}_1 P_1 + \cdots + \bar{y}_i P_i$ with $P_i \not\equiv 0$ and $i \leqslant n$. Let X_i be a first variable in $\bar{y}_i$ which is not a first variable in $\bar{y}_0, \bar{y}_1, \ldots, \bar{y}_{i-1}$. Let M be a monomial of lowest degree in $\bar{y}_i$ that has X_i as a first variable. Since degree $P_i <$ degree P, P_i is not zero on the $\bar{y}_j$'s. So after writing P_i in terms of the X's let N be any monomial of smallest degree in P_i in terms of the X's. Then MN will be a monomial in P that can be duplicated neither as a monomial in $\bar{y}_i P_i$ because of the minimality of the degrees of M and N nor as a monomial in $\bar{y}_j P_j$, $j < i$ because X_i is the first variable of MN. Thus P is not zero on $\bar{y}_0, \bar{y}_1, \ldots, \bar{y}_n$. Q.E.D.

Note that in the last part of the above we proved the following corollaries.

COROLLARY 2.10′. *With $\mathfrak{H}$ as above, the elements in any regular sequence in $\mathfrak{H}$ are algebraically independent.*

COROLLARY 2.11. *$\mathfrak{H}$ as in the proposition. Let $y_0, y_1, \ldots, y_n$ (n finite or infinite) be a regular sequence in $\mathfrak{H}$ and assume that there exists* GPIC-*subHopf algebras $\mathfrak{I}_0, \mathfrak{I}_1, \ldots, \mathfrak{I}_n$ such that $\Delta y_i = y_i \otimes 1 + 1 \otimes y_i + T_i$ with $T_i \in \mathfrak{I}_i \otimes \mathfrak{I}_i$ and such that $V(\mathfrak{I}_i)\ p\ \mathfrak{I}_{i-1}$, $i \geqslant 1$. Then there exists a standard sequence generated by $\bar{y}_0, \bar{y}_1, \ldots, \bar{y}_n$ with $\bar{y}_i$ of the form $y_i + z_i$, $z_i \in \mathfrak{I}_i$.*

Proof. By Proposition 2.5 there exists a primitive $\bar{y}_0$ of the form $y_0 + z_0$ with $z_0 \in \mathfrak{I}_0$. Now use induction and Proposition 2.10 to construct the rest of the standard sequence.

DEFINITION 2.12. Let $\mathfrak{C}$ be a PIC-coalgebra and $\{x_i\}_{i \in I}$ a basis homogeneous with respect to some filtration $\{\mathfrak{C}_i\}_{i=0}^{\infty}$. We place a partial ordering on the monomials in the canonical representation of $F(\mathfrak{C})$ as follows: Assign to each monomial M a vector $(a_1, a_2, a_3, \ldots)$ where a_i equals the sum of the exponents of the variables in M which are contained in $F(\mathfrak{C}_i) - F(\mathfrak{C}_{i-1})$. Order these vectors by Semitic lexicography (i.e., lexicographically from the right). Then $M < N$ if the vector corresponding to M is less than the vector corresponding to N.

LEMMA 2.13. (a) *If $N' \nleqslant N$ and $M < N$ then $M < N'$.*

(b) *If $M < N$ and $M' \ngtr N'$ then $MM' < NN'$.*

(c) *$V(M) < M$.*

(d) *If $\{\mathfrak{C}_i\}_{i=0}^{\infty}$ is the associated filtration of some grading of $\mathfrak{C}$, then if $V(M) \neq 0$ and if $M \not< N$, then $V(M) \not< V(N)$.*

Proof. The proofs of (a) and (b) are straightforward. (c) follows from [1.19] and (d) from [1.20].

DEFINITION 2.14. (a) If P is a polynomial in $F(\mathfrak{C})$, we say P is isogeneous if all the monomials in P are incomparable.

(b) If P and Q are two polynomials in $F(\mathfrak{C})$ we will say $P < Q$ if every monomial in P is less than every monomial in Q.

(c) If M, M', N, N' are monomials in $F(\mathfrak{C})$ then $M \otimes M' < N \otimes N'$ if $MM' < NN'$.

(d) Similarly $M \otimes M' < N$ if $MM' < N$. Note that no term in ΔN is larger than N.

LEMMA 2.15. *Let $\mathfrak{C}$ be a* PIC-*coalgebra and $\{x_i\}_{i \in I}$ a basis homogeneous with respect to some filtration. Let $\{P_i\}_{i \in J}$ be a set of polynomials in the canonical representation of $F(\mathfrak{C})$ and write each P_i as $Q_i + R_i$ with $Q_i > R_i$ and Q_i isogeneous. Then the P_i are algebraically independent if the Q_i are.*

Proof. Let f be a polynomial in the P_i's such that $f(P_i)_{i\in J} = 0$. Part (b) of Lemma 2.13 insures that all the monomials in $f(P_i)$ that appear in $f(Q_i)$ will be larger than the monomials in $f(P_i)$ not in $f(Q_i)$. Thus, $f(Q_i) = 0$ which means that f was trivial.

THEOREM 2.16. *Let $\mathfrak{C}$ be a* PIC*-coalgebra with a regular basis $\mathfrak{B}$ that is also homogeneous with respect to some filtration $\{\mathfrak{C}_i\}_{i=0}^{\infty}$. Then $F(\mathfrak{C})$ is isomorphic to the coproduct of P_i's with the number of P_n's in the coproduct equal to the number of regular sequences of length n in $\mathfrak{B}$. (The coproduct in the category of Hopf algebras is the free product. The coproduct in the category of commutative Hopf algebras is the tensor product.)*

Proof. Note that since $\mathfrak{B}$ is homogeneous, if X_i is a variable in the canonical representation of $F(\mathfrak{C})$ and $X_i \in F(\mathfrak{C}_{r_i+1}) - F(\mathfrak{C}_{r_i})$ then

$$\Delta X_i = 1 \otimes X_i + X_i \otimes 1 + T \qquad \text{with} \quad T \in F(\mathfrak{C}_{r_i}) \otimes F(\mathfrak{C}_{r_i}).$$

Now pick any regular sequence $X_0, X_1, \ldots, X_n$ among the variables. Assume $X_i \in F(\mathfrak{C}_{r_i+1})$ and let $\mathfrak{J}_i'$ be the Hopf algebra generated by X_i and let $\mathfrak{J}_i = \mathfrak{J}_i' \cap F(\mathfrak{C}_{r_i})$. Note that $\mathfrak{J}_{i-1} \subset V(\mathfrak{J}_i)$, for $V(X_i) = X_{i-1}$ implies $\mathfrak{J}_{i-1}' \subset V(\mathfrak{J}_i')$ and if monomial $M \in \mathfrak{J}_i' - \mathfrak{J}_i$, M contains X_i which means that $V(M)$ contains X_{i-1} or equals zero, i.e., $V(M) \neq 0$ implies $V(M) \in \mathfrak{J}_{i-1}' - \mathfrak{J}_{i-1}$. Consequently, if $N \in \mathfrak{J}_{i-1}$ and $V^{-1}(N) \cap \mathfrak{J}_i' \neq \varnothing$, then $V^{-1}(N) \cap \mathfrak{J}_i \neq \varnothing$.

Now apply Corollary 2.11 to obtain a standard sequence whose ith generator is of the form $X_i + P_i$ with $P_i \in F(\mathfrak{C}_{r_i})$ (note, $X_i > P_i$). By definition, the Hopf algebra generated by this standard sequence is isomorphic to $\mathfrak{P}_n$.

Thus, if we follow this procedure for all regular sequences among the variables we obtain a set of polynomials which are algebraically independent (by Lemma 2.15). Further they generate, as an algebra, all of $F(\mathfrak{C})$. For let $\mathfrak{M}$ be the algebra generated by them. Trivially $F(\mathfrak{C}_0) \subset \mathfrak{M}$. Assume inductively that $F(\mathfrak{C}_r) \subset \mathfrak{M}$ and let $X_i \in F(\mathfrak{C}_{r+1}) - F(\mathfrak{C}_r)$. Then we have a generator $X_i + P_i$ with $P_i \in F(\mathfrak{C}_r)$, which means that $X_i \in \mathfrak{M}$. Q.E.D.

The following propositions show that many classes of PIC-coalgebras have regular homogeneous bases.

PROPOSITION 2.17. *Let $\mathfrak{C}$ be a* PIC*-coalgebra and assume there exists an N such that $V^N(\mathfrak{C}) = \langle \mathfrak{R}g \rangle$. Then with respect to any filtration $\{\mathfrak{C}_i\}_{i=0}^{\infty}$ of $\mathfrak{C}$ (and there is at least one,* [1.11]*) $\mathfrak{C}$ has a regular homogeneous basis.*

Proof. We will use that notation $V^{n-1}(\mathfrak{C}[i_1, \ldots, i_n])$ for

$$(\underbrace{V \cdots V}_{n-1}(V(\mathfrak{C}_{i_1}) \cap \mathfrak{C}_{i_2}) \cap \cdots \cap \mathfrak{C}_{i_{n-1}}) \cap \mathfrak{C}_{i_n}$$

and when convenient let $\mathfrak{C}_\infty = \mathfrak{C}$.

Start with g and (adding elements in $\ker \epsilon$) extend to a basis of $V^{N-1}(\mathfrak{C}[1, 1,..., 1])$ then to a basis of $V^{N-1}(\mathfrak{C}[2, 1,..., 1])$, etc. until we have a basis of $V^{N-1}(\mathfrak{C}[\infty, 1,..., 1])$. Now adjoin to this basis an extension to $V^{N-1}(\mathfrak{C}[1, 2, 1,..., 1])$ (i.e., obtain a basis of $V^{N-1}(\mathfrak{C}[\infty, 1,..., 1]) + V^{N-1}(\mathfrak{C}, 2,..., 1])$ then extend to $V^{N-1}(\mathfrak{C}[2, 2, 1,..., 1])$ etc. until we have a basis of $V^{N-1}(\mathfrak{C}[\infty, 2, 1,..., 1])$. Now in a like manner find a basis of $V^{N-1}(\mathfrak{C}[\infty, 3, 1,..., 1])$, etc. until we have a basis of $V^{N-1}(\mathfrak{C}[\infty, \infty, 1,...,1])$. Now start with the third subscript. Eventually we obtain a basis of $V^{N-1}(\mathfrak{C})$. (Note: Since $V(\mathfrak{C}_n) \subset \mathfrak{C}_{n/p}$ it is only for convenience that we start with $\mathfrak{C}[1, 1,..., 1]$ instead of $\mathfrak{C}[p^N,..., p^0]$.)

Now extend this basis to a basis of $V^{N-2}(\mathfrak{C})$ constructed in a parallel manner, except that at each step first look at $V(V^{N-2}(\mathfrak{C}[i_1,..., i_{N-1}]))$. From the method of construction of the basis of $V^{N-1}(\mathfrak{C})$, we know that there exists a subset of that basis which extends V of the part of $V^{N-2}(\mathfrak{C})$ that we have already considered to $V(V^{N-2}(\mathfrak{C}[i_1,..., i_{N-1}])$. (It will be the union over m of the extensions made when forming a basis for $V^{N-1}(\mathfrak{C}[i_1,..., i_{N-1}, m])$.) For each element in that extension find a preimage in $V^{N-2}(\mathfrak{C}[i_1,..., i_{N-1}])$. Then adjoin elements in $\ker V$ to get a basis of $V^{n-2}(\mathfrak{C}[i_1,..., i_{N-1}])$. (This is possible by Proposition 2.2.)

The generalization to the construction of a basis of $V^i(\mathfrak{C})$ is clear and the basis we will obtain is both regular and homogeneous.

PROPOSITION 2.18. *Let $\mathfrak{C}$ be a* GPIC*-coalgebra with a grading $\{\mathfrak{D}_i\}_{i=0}^{\infty}$. Then $\mathfrak{C}$ has a regular basis which is homogeneous (and therefore homogeneous with respect to the associated filtration)*:

LEMMA 2.19. *Let V be a vector space with q sequence of subspaces $V = V_0 \supset V_1 \supset V_2 \supset \cdots \supset V_\infty$ such that $\bigcap_{n<\infty} V_n = V_\infty$. Assume V has a basis $\{x_i\}_{i\in I}$ which for any n contains a subset which is a basis of V_n. Then if W is a subspace of V, W has a similar basis with respect to $W_0 \supset W_1 \supset W_2 \supset \cdots \supset W_\infty$ where $W_n = V_n \cap W$.*

Proof. Assume initially that $\bigcap_{n<\infty} V_n = 0$. Let $\{y_i\}_{i\in J}$ be a basis of W and let A_n be the subspace of V generated by $\{x_i \mid x_i \in B \text{ and } x_i \in V_n - V_{n+1}\}$. Then by hypothesis $V = \oplus_n A_n$, so write each y_i as $\sum_j a_{ij}$ with $a_{ij} \in A_j$. Now place a well ordering on J with the priviso that $j < i$ if $y_j \in \oplus_{n=1}^{m} A_n$ and $y_i \notin \oplus_{n=1}^{m} A_n$ for some m.

Let $E_0 = \{i \in J \mid a_{i0} \text{ is independent of } \{a_{j0} \mid j < i\}\}$. Note that $\{a_{i0} \mid i \in E_0\}$ forms a basis of the space spanned by $\{a_{i0} \mid i \in J\}$. (If not, there must exist a least $j \ni a_{j0}$ is not in the space. Contradiction.) So for each $y_i \ni i \notin E_0$ we can eliminate the a_{i0} term by taking a proper linear combination of $\{y_j \mid j \in E_0$ and $j < i\}$ and subtracting from y_i. Continue to call this changed term y_i.

Now with respect to these new y_i's let $E_1 = \{i \in j - E_0 \mid a_{i1}$ is independent of $\{a_{j1} \mid j < i,\ j \notin E_0\}\}$. Again eliminate all the a_{i1} terms in $y_i \ni i \in J - (E_0 \cup E_1)$ and get new y_i's. Similarly define E_2, etc.

Note that $\bigcup E_i = J$, because pick $i \in J$ and assume the initial $y_i \in \bigoplus_{n=1}^{m} A_n$. Then at each step if $i \notin E_t$, a linear combination of elements smaller than y_i is subtracted from y_i. Thus the changed y_i will still be in $\bigoplus_{n=1}^{m} A_n$. Consequently, if $i \notin \bigcup_{n=1}^{m-1} E_n$, by the mth step $y_i = a_{im}$. Similarly $y_j = a_{jm}$ $\forall\{j \mid j < i$ and $j \notin \bigcup_{n=1}^{m-1} E_n\}$. Thus if $i \notin E_m$, y_i is dependent on previous y_j's, which would imply, if we work backwards, that the original basis of W was not independent.

Note, too, that the changed y_i's still span W, since we can write each original y_i as a linear combination of the changed ones.

Finally, the final basis is of the correct form, for consider $\sum b_i y_i$, a linear combination of final basis elements, and assume at least one i is in E_m but none in $\bigcup_{n=1}^{m-1} E_n$. Then since the final $\{a_{im}\}$ are independent $\sum b_i y_i \in V_n - V_{n+1}$, i.e., in order to write any element in W_{n+1} in terms of the final basis one can only use basis elements in W_{n+1}. Thus $\{y_i \mid i \in \bigcup_{n=m}^{\infty} E_n\}$ will be a basis for W_m.

Now drop the assumption that $\bigcap_{n<\infty} V_n = 0$. Clearly V/V_∞ has a "good" basis with respect to $V_0/V_\infty \supset V_1/V_\infty \supset \cdots$, so W/W_∞ also has such a basis. Since $W \approx W_\infty \oplus W/W_\infty$ the basis of W/W_∞ plus a basis of W_∞ will be the desired basis of W.

Proof of Proposition. By the lemma, for each n we can find a basis of $D_n \cap \ker V$ which contains $\forall m$ a basis of $V^m(\mathfrak{C}) \cap (D_n \cap \ker V)$. The union of these bases will be a homogeneous coalgebra Sweedler basis. Now in constructing our regular basis, assume we already have a regular sequence of homogeneous elements ${}_0x_i, {}_1x_i, {}_2x_i, \ldots, {}_{n-1}x_i$ with ${}_0x_i$ in the coalgebra Sweedler basis and (coheight ${}_jx_i$) + 1 = coheight ${}_{j-1}x_i$. If $V(y) = {}_{n-1}x_i$ and coheight y = (coheight ${}_{n-1}x_i$) − 1, let ${}_nx_i$ be the pt component of y if degree of ${}_{n-1}x_i = t$. Proposition 2.2 implies that the totality of these regular sequences together with g forms a basis of $\mathfrak{C}$.

PROPOSITION 2.20. *If $\mathfrak{H}$ is a* GPIC*-Hopf algebra then $\mathfrak{H}$ has a regular basis, homogeneous with respect to some filtration.*

Proof. Using the basis of [1.30] and using the normal diagonalization, it is clear that we can put a coalgebra grading on $\mathfrak{H}$ with degree of $\prod {}^{n_i}x_i = \sum n_i$. As remarked in [2.3] this basis is regular.

Remarks. 2.21. (a) Though many aspects of coheight theory and SDP theory apply to Hopf algebras over nonperfect fields (see [5]), [5, Example 2, p. 30] indicates that Sweedler's structure theorem is not true. The same

example shows that Theorem 2.16 also is not true. For if $\mathfrak{C}$ is the Hopf algebra described there, $F(\mathfrak{C})$ cannot, on the one hand, be a coproduct of $\mathfrak{P}_0$'s since $V(F(\mathfrak{C})) \neq 1 \otimes \mathfrak{K}^{1/p}$, and, on the other hand, cannot have any $\mathfrak{P}_n$'s, $n > 0$, in the coproduct since no element of $F(\mathfrak{C})$ has coheight 1.

(b) Theorem 2.16 is also not true without the assumption that $V(V^\infty(\mathfrak{C})) = \mathfrak{C}$. For let $\mathfrak{C}$ be the Hopf algebra described in [5, Example 1, p. 27]. Then $F(\mathfrak{C})$ has variables of infinite coheight, (i.e., $V^\infty(F(\mathfrak{C}))$ is non-trivial) though $V(V^\infty(F(\mathfrak{C}))$ is trivial. But in general $V(V^\infty(\coprod \mathfrak{P}_i)) = V^\infty(\coprod \mathfrak{P}_i)$. Therefore, $F(\mathfrak{C})$ is not isomorphic to $\coprod \mathfrak{P}_n$.

3

Theorem 2.16 indicates that over perfect fields $\mathfrak{P}_n$ has some of the properties of projectives in the category of GPIC-Hopf algebras. (Actually, in the category of *graded* Hopf algebras, if we let degree of $Y_i = 2p^i$, they *are* projectives. See [6'].) It is natural, therefore, to consider the structure of the categorical kernel of $\varphi: F(\mathfrak{H}) \to \mathfrak{H}$. (The map, of course, consists of mapping the variables of $F(\mathfrak{H})$ to their corresponding basis element of $\mathfrak{H}$.) Theorem 3.8 shows that when $\mathfrak{H}$ is a GPIC-Hopf algebra, it is also a coproduct of $\mathfrak{P}_n$'s.

DEFINITION 3.1. If $\varphi: \mathfrak{H} \to \mathfrak{J}$ is a map of cocommutative Hopf algebras, then let $H\text{-ker}\,\varphi$ be the set: $\{x \in \mathfrak{H} \mid (\varphi \otimes I)\,\Delta x = 1 \otimes x\}$.

[8, Lemma 16.1.1, pp. 312–313] shows that $H\text{-ker}\,\varphi$ is a subHopf algebra of $\mathfrak{H}$. It is easy to see that $H\text{-ker}\,\varphi$ is the kernel of φ in the category of cocommutative Hopf algebras.

It is well known that if $\mathfrak{U}$ is an associative algebra over a field of characteristic p, $\mathfrak{U}$ can be given a restricted Lie algebra structure via $x \circ y = xy - yx$ and $x^{[p]} = x^p$ [4, p. 188]. In the following, when we talk of restricted Lie algebras contained in associative algebras, we will assume that the restricted Lie algebra structure is of this form.

DEFINITION 3.2. If $\mathfrak{K}[X_i]_{i\in I}$ is a polynomial ring (commutative or non-commutative) an element of the form $X_{i_1} \circ X_{i_2} \circ \cdots \circ X_{i_n}$ (associated in any order) or the p^nth power of such an element, will be called *basal* or, alternatively, *basal with respect to* $\{X_i\}_{i\in I}$.

Note that if $F(\mathfrak{C})$ is the canonical representation of a PIC-coalgebra with a homogeneous basis, all basal elements are isogeneous.

LEMMA 3.3. *Any element in the restricted Lie algebras generated by the variables of* $\mathfrak{K}[X_i]_{i\in I}$ *is a linear combination of basal elements.*

Proof. The lemma follows immediately from

$$a \circ b^p = (\cdots (a \circ \overbrace{b) \circ b) \circ \cdots \circ b}^{p})$$

[4, p. 186] and $(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} s_i(a, b)$ with $s_i(a, b)$ in the Lie algebra generated by the a and b [4, p. 187].

PROPOSITION 3.4. *Let $\mathfrak{C}$ be a* PIC*-coalgebra and $\{x_i\}_{i\in I}$ a regular homogeneous basis of $\mathfrak{C}$ with respect to some filtration $\{\mathfrak{C}_i\}_{i=0}^{\infty}$. Let $\mathfrak{S} = \{P_i\}_{i\in J}$ be a set of isogeneous polynomials in the canonical representation of $F(\mathfrak{C})$. Assume that if $P_i \in \ker V^{n_i+1} - \ker V^{n_i}$, we have generators of a standard sequence ${}_0P_i, {}_1P_i, \ldots, {}_{n_i}P_i$ where ${}_jP_i = V^{n_i-j}(P_i) + {}_jQ_i$ with ${}_jQ_i < V^{n_i-j}(P_i)$.*

Now let T be any isogeneous element contained in $\mathfrak{L}$, the restricted Lie algebra generated by the elements of $\mathfrak{S}$. If $T \in \ker V^{m+1} - \ker V^m$, then there exists an mth generator $\bar{T}$ of some standard sequence such that $\bar{T} = T + U$ with $U < T$ and such that $\bar{T}, V(\bar{T}), \ldots, V^m(\bar{T})$ are in the algebra generated by the ${}_jP_i$'s.

Further, if for each i, each monomial in P_i contains the same variables and coheight ${}_nP_i$ = coheight P_i, and $T \in \ker V$, then we can pick $\bar{T}$ (here a primitive) such that coheight T = coheight $\bar{T}$.

Proof. First we show that if P and P' are in $\mathfrak{S}$, then we can find $\bar{T}$ for (a) $P \circ P'$, (b) P^p, (c) $P + P' (P \lesseqgtr P')$, and (d) aP, $a \in \mathfrak{K}$.

(a) Put a Hopf algebra bigrading on $\mathfrak{C} = \mathfrak{K}[{}_0P, \ldots, {}_nP, {}_0P', \ldots, {}_mP']$ via $\deg_i P = (p^i, 0)$ and $\deg_i P' = (0, p^i)$. Assume $m \leqslant n$ and consider ${}_{n-m}P \circ {}_0P'$. If $m < n$ consider $\mathfrak{F} = \mathfrak{K}[{}_0P, \ldots, {}_{n-m-1}P, {}_0P']$. Note that $\Delta({}_{n-m}P \circ {}_0P') = 1 \otimes {}_{n-m}P \circ {}_0P' + {}_{n-m}P \circ {}_0P' \otimes 1 + R$ where $R \in \mathfrak{F} \otimes \mathfrak{F}$. Thus by Proposition 2.5 there exists a primitive of the form ${}_{n-m}P \circ {}_0P' + S$ with $S \in \mathfrak{F}$. Clearly the $(p^{n-m}, 1)$ homogeneous component of this primitive will still be a primitive, which we will call ${}_0T$.

If $n = m$, then ${}_{n-m}P \circ {}_0P$ is automatically the ${}_0T$ we are looking for.

Assume inductively that we have generators of a standard sequence ${}_0T, {}_1T, \ldots, {}_jT$ such that ${}_iT$ is homogeneous of $\deg(p^{n-m+i}, p^i)$ and ${}_jT$ contains ${}_{n-m+i}P \circ {}_iP$ with coefficient 1. Then by Lemma 1.26, $\exists$ in $\mathfrak{C}$ a $(j+1)$st generator ${}_{j+1}T$ of the above sequence. We can assume ${}_{j+1}T$ is homogeneous of degree $(p^{n-m+j+1}, p^{j+1})$. Since $V({}_{j+1}T) = {}_jT$, ${}_{j+1}T$ must contain ${}_{n-m+1+j}P \circ {}_{j+1}P$ with coefficient 1.

Thus we can obtain $\bar{T}$, homogeneous of degree (p^n, p^m) containing ${}_nP \circ {}_mP'$. By degree consideration $\bar{T}$ can contain no other monomial containing both ${}_nP$ and ${}_mP'$ or any monomial containing higher powers of ${}_nP$ or ${}_mP'$.

Now thinking in terms of $F(\mathfrak{C})$, by Lemma 2.13 (c), every monomial in ${}_0P, \ldots, {}_{n-1}P$ is less than P and, in fact, every variable in ${}_0P, \ldots, {}_{n-1}P$ is less than

the largest variable in P. A similar statement holds for P'. Thus in $\bar{T}$, the largest variables can appear only in monomials containing both ${}_nP$ and ${}_mP'$, i.e., in ${}_nP \circ {}_mP'$, and by Lemma 2.13 (b) the largest monomial in ${}_nP \circ {}_mP'$ is $P \circ P'$. Thus $\bar{T}$ is of the correct form.

(b) As noted in [2.6] we can put a Hopf algebra grading on $\mathfrak{M} = \mathfrak{K}[{}_0P, {}_1P, \ldots, {}_mP]$ with $\deg {}_jP = p^j$. Now P_0 a primitive implies ${P_0}^p$ is a primitive and since $V^m({}_mP^p) = {}_0P^p$, we can assume there exists in $\mathfrak{M}$ a standard sequence whose 0th generator is ${}_0P^p$ and mth generator is Q, with Q homogeneous of degree p^{m+1}. Since $V^m(Q) = {}_0P^p$, Q must contain the monomial ${}_mP^p$ and since it is homogeneous ${}_mP^p$ will be the largest monomial (in terms of $\mathfrak{M}$) which implies the monomial P^p in ${}_mP^p$ will be the largest monomial in Q in terms of $F(\mathfrak{C})$.

(c) is proved similarly to (a) and (b).

(d) is trivial.

Now assume T is of the form $(P_{i_1} \circ P_{i_2} \circ \cdots \circ P_{i_n}) \circ P_{i_m}$. Let

$$\mathfrak{C}' = \{(P_{i_1} \circ P_{i_2} \circ \cdots \circ P_{i_n}), P_{i_m}\}.$$

By induction we can assume we can find a generator of a standard sequence of the proper form for $P_{i_1} \circ P_{i_2} \circ \cdots \circ P_{i_n}$. Then replacing $\mathfrak{S}$ by $\mathfrak{S}'$, part (a) of the above proves the theorem for T.

Similarly if T is of the form $(P_{i_1} \circ P_{i_2} \circ \cdots \circ P_{i_n})^{p^t}$, $t \geqslant 1$, we can assume we have proved the theorem for $(P_{i_1} \circ P_{i_2} \circ \cdots \circ P_{i_n})^{p^{t-1}}$ and use part (b) of the above.

Finally, if T is an arbitrary element in the restricted Lie algebra generated by $\mathfrak{S}$, the lemma tells us we can write T as a linear combination of basal elements (in terms of $\mathfrak{S}$). Use parts (c) and (d) and induction to complete this part of the proof.

The last paragraph of the theorem can be proved by noting that under the additional hypothesis, every element in $\mathfrak{K}[{}_0P, {}_1P, \ldots, {}_nP, {}_0P', {}_1P', \ldots, {}_mP']$ has coheight greater than or equal to min {coheight P, coheight P'}. But this is also the coheight of $P \circ P'$, by Remark 2.4 (if P and P' do not commute). Thus, the generator of a standard sequence we select for (nontrivial) $P \circ P'$ has the same coheight as $P \circ P'$. A similar argument proves the corresponding result for P^p, and now induction shows that if S is basal in terms of $\mathfrak{S}$, $\exists$ a $\bar{S}$ of the form $S + R$ with $R < S$ and coheight $\bar{S}$ = coheight S.

Now assume $T \in \ker V$ and $T = \sum a_i S_i$, $a_i \in \mathfrak{K}$ and each S_i basal in terms of $\mathfrak{S}$ and linearly independent. Since each monomial in each P_i contains the same variables, each monomial in each S_i contains the same variables. Then

the regularity of the variables implies that the nonzero $V(S_i)$ are linearly independent. Thus each $S_i \in \ker V$. Similarly, Remark 2.4 implies that coheight $S_i \geqslant$ coheight T, $\forall i$. Now for each i pick a $\bar{S}_i$ by the above procedure. Then since each $\bar{S}_i$ is a primitive, $\sum a_i \bar{S}_i$ will be the desired $\bar{T}$.

LEMMA 3.5. *Give the commutative or noncommutative polynomial ring* $\mathfrak{K}[X_i]_{i\in I}$ *a Hopf algebra structure by letting each* X_i *be a primitive. Then* $\mathscr{P}(\mathfrak{K}[X_i]_{i\in I}) = \mathfrak{L}$ *(the restricted Lie algebra generated by the* X_i*'s).*

Proof. Since X, Y primitives implies that $X \circ Y$, X^p and $aX + bY$ ($a, b \in \mathfrak{K}$) are primitives, clearly $\mathfrak{L} \subset \mathscr{P}(\mathfrak{K}[X_i]_{i\in I})$.

The converse parrots [4, Theorem 9, p. 170].

COROLLARY 3.6. *Let* $\{x_i\}_{i\in I}$ *be a regular, homogeneous basis with respect to some filtration* $\{\mathfrak{C}_i\}_{i=0}^{\infty}$ *of a* PIC*-coalgebra* $\mathfrak{C}$. *Let* P, *a polynomial in the canonical representation of* $F(\mathfrak{C})$, *be a generator in a standard sequence. Then if* P' *represents the largest monomials in* P, $P' \in \mathfrak{L}$, *the restricted Lie algebra generated by the variables in* $F(\mathfrak{C})$.

Proof. Let M be a monomial in P' and X a variable in M. As $\{x_i\}_{i\in I}$ is homogeneous $\Delta X = 1 \otimes X + X \otimes 1 + U$ with $U \in F(\mathfrak{C}_r) \otimes F(\mathfrak{C}_r)$ if $X \in F(\mathfrak{C}_{r+1}) - F(\mathfrak{C}_r)$. As we construct any of the largest terms in ΔM by multiplying the diagonalizations of the variables in M, when we multiply by a term in ΔX we must use $1 \otimes X$ or $X \otimes 1$ since multiplying by any term in U will yield a smaller product. Further, it is clear that all the largest terms in ΔP are actually terms in $\Delta P'$.

So assume that in $\Delta P'$ one of the largest terms is $K \otimes L$. Then if $P' \in F(\mathfrak{C}_{r+1}) - F(\mathfrak{C}_r)$, either K or L are in $F(\mathfrak{C}_{r+1}) - F(\mathfrak{C}_r)$. But P is a generator of a standard sequence, which implies that

$$\Delta P = P \otimes 1 + 1 \otimes P + W,$$

with $W \in \mathfrak{J} \otimes \mathfrak{J}$ ($\mathfrak{J}$ = Hopf algebra generated by $V(P)$). Since $V(P) \subset F(\mathfrak{C}_s)$, $s =$ greatest integer $\leqslant (r+1)/p$ [1.19], we have that K or L equals 1 and $\Delta P' = 1 \otimes P' + P' \otimes 1 + T$ with $T < P'$. Consequently, if we change the diagonalization of each variable of P' so that it is a primitive $\Delta P' = 1 \otimes P' + P' \otimes 1$. (Clearly the diagonalization of a product of isogeneous primitives is isogeneous.) Thus by the lemma, $P' \in \mathfrak{L}$. Q.E.D.

Before proceeding, we need some facts about free restricted Lie algebras.

First, if $\mathfrak{F} = \{X_i\}_{i\in I}$, we can construct a free restricted Lie algebra on $\mathfrak{F}$ over $\mathfrak{K}$ in the following way. Take the noncommutative polynomial ring on $\mathfrak{F}$ and give it a restricted Lie algebra structure in the standard way. Then the

free restricted Lie algebra on $\mathfrak{F}$ will be the restricted Lie algebra generated by the variables. This can be proved in the same way as the corresponding statement for free Lie algebras. For the latter see [4, p. 167].

Second, we need some results of Witt [10] about subrestricted Lie algebras of free restricted Lie algebras. We summarize, in severely edited form, the relevant parts of his paper. (See also a useful summary in [1].)

Let $\mathfrak{L}$ be a free restricted Lie algebra, and let $X = \{x_i\}_{i\in I}$ be a set of free generators. Let $x_i \to |x_i|$ be a map of the generators into an ordered commutative group $\mathfrak{S}$ such that $|x_i| >$ (the identity) $\forall i$. (We will take $\mathfrak{S}$ to be the additive integers, but written multiplicatively, to conform to Witt's notation, and let $|x_i| = 1$ $\forall i$.) Let $\mathfrak{A}$ be the restricted universal enveloping algebra of $\mathfrak{L}$ ($\mathfrak{A}$ will equal $\mathfrak{K}[x_i]_{i\in I}$) and thinking of $\mathfrak{L} \subset \mathfrak{A}$, define X_s, the subspace of $\mathfrak{A}$ spanned by the products $x_1x_2 \cdots x_n$, $n \geqslant 0$, $x_i \in X$, $\prod |x_i| \leqslant s$. Now let $\mathfrak{U}$ be an arbitrary subrestricted Lie algebra of $\mathfrak{L}$ and define $\mathfrak{U}_s = \mathfrak{U} \cap X_s$ and $\mathfrak{B}_s = \mathfrak{U} \cap \sum \mathfrak{U}_{t_1} \cdots \mathfrak{U}_{t_n}$ summing over t_i's such that $t_i < s$, $\prod t_i \leqslant s$. Then if we take a basis of $\mathfrak{U}_s$ mod $\mathfrak{B}_s$, for each s, the union of these bases will be a free generating set of $\mathfrak{U}$, or, in particular, $\mathfrak{U}$ is a free restricted Lie algebra [10, pp. 197, 203 and Hauptsatz, p. 205].

PROPOSITION 3.7. *Let $\mathfrak{C}$ be a* PIC*-coalgebra with regular basis $\{x_i\}_{i\in I}$. Let $\mathfrak{L}$ be the free restricted Lie algebra generated by the variables in the canonical representation of $nF(\mathfrak{C})$. Now let $\mathfrak{U}$ be a subrestricted Lie algebra of $\mathfrak{L}$. Assume $\mathfrak{U}$ has a regular set of linearly independent generators $\mathfrak{F}$ consisting of basal elements, with the property that if $y \in \mathfrak{F}$ and $y \in V^n(\mathfrak{U})$ then y is in $V^n(\mathfrak{F})$ and if $V^n(y) \in \mathfrak{B}_S$ then $y \in \mathfrak{B}_S$. Then $\mathfrak{U}$ has a regular free generating set consisting of basal elements.*

Proof. We will construct for each s a regular basis of $\mathfrak{U}_s$ mod $\mathfrak{B}_s$ consisting of basal elements. The above remarks will then complete the proof.

First, pick an arbitrary basis $\mathfrak{G} = \{z_i\}_{i\in J}$ $\mathfrak{U}_s$ mod $\mathfrak{B}_s$. By Lemma 3.3 we can write each z_i as $\sum_j a_{ij}y_{ij}$ with $a_{ij} \in \mathfrak{K}$ and y_{ij} basal in terms of $\mathfrak{F}$ and linearly independent. Since z_i is a polynomial of degree s, each y_{ij} is a polynomial of degree $\leqslant s$, i.e., each y_{ij} is in $\mathfrak{U}_s$. Thus, if y_{ij} is not in $\mathfrak{F}$, then it is a commutator or pth power of elements of $\mathfrak{F}$, i.e., $y_{ij} \in \mathfrak{B}_s$. Such terms can be dropped from the sum without affecting the fact that $\mathfrak{G}$ is a basis for ($\mathfrak{U}_s$ mod $\mathfrak{B}_s$). Consequently, we can assume each $y_{ij} \in \mathfrak{F}$ and in $\mathfrak{U}_s - \mathfrak{B}_s$. Thus, a subset $\mathfrak{G}'$ of the y_{ij}'s form a basis for $\mathfrak{U}_s$ mod $\mathfrak{B}_s$.

Now $\mathfrak{F}$ is a regular, linearly independent set, and thus if a linear combination of elements of $\mathfrak{G}'$ are in ker V, each of the terms in the linear combination must be in ker V. Thus, we can pick $\mathfrak{G}''$, a subset of $\mathfrak{G}'$, as a basis for ($\mathfrak{U}_s$ mod $\mathfrak{B}_s$) $\cap$ ker V.

Now for each element of $\mathfrak{G}''$ pick the regular sequence in $\mathfrak{F}$ that contains it. It is clear that each of these elements is in $\mathfrak{U}_s$. The proof that they form a

basis for $\mathfrak{U}_s \bmod \mathfrak{B}_s$ is very similar to the proof of Proposition 2.2 and will not be repeated. Q.E.D.

THEOREM 3.8. *Let $\mathfrak{H}$ be a* GPIC-*Hopf algebra with Sweedler basis $\mathfrak{B} = \{y_i\}_{i\in I}$. Then the Hopf kernel of $\varphi: F(\mathfrak{H}) \to \mathfrak{H}$ is the coproduct of $\mathfrak{P}_n$'s* [*Definition* 2.6]. (*If $\mathfrak{H}$ is not commutative, consider only $nF(\mathfrak{H})$; otherwise φ will not be a Hopf algebra map.*)

Proof. Let $\mathfrak{E} = \{z_i\}_{i\in J}$ be a regular basis of $\mathfrak{H}$ of the type described in [1.30]. Place on $\mathfrak{H}$ the grading described in Corollary 2.20, and consider $\mathfrak{H}$ filtered by its associated filtration. As noted in [2.20], $\mathfrak{E}$ will be a homogeneous basis.

In the canonical representation of $F(\mathfrak{H})$, let $\mathfrak{T}$ be the set containing those variables that correspond to elements in $\mathfrak{E}$ which are p^nth elements in their SDP (i.e., in the notation of [1.30], correspond to monomials of the form: ${}^{p^n}x_i$, $n = 0, 1,\ldots$). Let $\mathfrak{U}$ be the restricted Lie algebra generated by (1) the variables of $F(\mathfrak{H})$ not in $\mathfrak{T}$, (2) elements of the form $X_{i_1} \circ X_{i_2} \circ \cdots \circ X_{i_n}$ (associated in any order), each X_{i_j} a variable in $F(\mathfrak{H})$ and $n \geqslant 2$ ((2) only relevant for $nF(\mathfrak{H})$), and (3) pth powers of elements in $\mathfrak{T}$.

In the noncommutative case, it is straightforward to see that we can pick a subset of the generators of $\mathfrak{U}$ that will satisfy the hypothesis of Proposition 3.7.

Thus $\mathfrak{U}$ has a regular free generating set consisting of basal elements. Call it $\mathfrak{F}$.

In the commutative case, we let $\mathfrak{F}$ equal all the variables in $F(\mathfrak{H})$ not in $\mathfrak{T}$ together with the pth power of all the variables in $\mathfrak{T}$. Again $\mathfrak{F}$ is a regular free generating set consisting of basal elements.

As in Theorem 2.16, for every variable X in $F(\mathfrak{H})$, such that $X \in \ker V^{n+1} - \ker V^n$, we can find an nth generator of a standard sequence of the form $X + R$, with $R < X$ and coheight $(X + R) =$ coheight R. Thus, by Proposition 3.4, if $P \in \mathfrak{F} \cap \ker V$, there exists a primitive $\bar{P}$ of the form: $P + Q$ with $Q < P$ and coheight $\bar{P} =$ coheight P. Now $\varphi(\bar{P}) \in \mathscr{P}(\mathfrak{H})$, and since φ is onto, coheight $\bar{P}$ in $F(\mathfrak{H})$ equals coheight $\varphi(\bar{P})$ in $\mathfrak{H}$. Therefore, $\varphi(\bar{P}) = \sum a_i y_i$, $a_i \in \mathfrak{K}$, $y_i \in \mathfrak{B}$ with the same coheight as $\bar{P}$. Since $\mathfrak{B} \subset \mathfrak{E}$, there is a variable Y_i in $F(\mathfrak{H})$ corresponding to each y_i. Then, if $P_0 = \bar{P} - \sum a_i Y_i$, P_0 is a primitive and equals $P + Q - \sum a_i Y_i$, where $Q - a_i Y_i < P$ and $\varphi(P_0) = 0$. Further, it follows directly from the definition of Hopf kernel, that primitives in the vector space kernel are in the Hopf kernel.

Now assume P is an arbitrary element of $\mathfrak{F}$ with $P \in \ker V^{n+1} - \ker V^n$, $n \geqslant 1$. Let coheight $P = t$. Since $\mathfrak{F}$ is regular, we can assume by induction that $\forall r \ni 0 \leqslant r < n$, there exists a polynomial $P_r = V^{(n-r)}(P) + Q_r$ such that

(1) $V^{(n-r)}(P) > Q_r$,

(2) $Q_r \in V^{(t-r+n)}(F(\mathfrak{H}))$ (the coheight of $V^{(n-r)}(P)$ is $t - r + n$),

(3) P_r, $r = 0, 1, \ldots, n-1$ are rth generators of the same standard sequence,

(4) $P_r \in H\text{-ker } \varphi$.

Using induction hypotheses 2 and 3, Proposition 2.10 says that there exists a $\bar{P}$ and an nth generator of the standard sequence, where $\bar{P} = P + R$ with $R \in V^t(F(\mathfrak{H}))$. (We are letting the $\mathfrak{F}$ in 2.10 equal $V^t(F(\mathfrak{H}))$. Note that $P \in \mathfrak{F}$.) If $P \not> R$, let N be the sum of the largest monomials in $\bar{P}$. (If N and P are incomparable, replace N by $N - P$.) Since $V(\bar{P}) = P_{n-1} = V(P) + Q_{n-1}$ with $Q_{n-1} < V(P)$, Lemma 2.13(d) implies that $V(N) = 0$. Thus, by Corollary 3.6, $N \in \mathfrak{L}$, the restricted Lie algebra generated by the variables of $F(\mathfrak{H})$. Proposition 3.4 now implies that there exists a primitive $\bar{N}$ of the form $N + M$ with $M < N$, and coheight $\bar{N}$ = coheight N. Note that $\bar{P} - \bar{N}$ still satisfies (2) and (3) of the induction hypothesis and, in addition, either $\bar{P} - \bar{N}$ satisfies (1) or $\bar{P} - \bar{N} < \bar{P}$. If (1) is not satisfied, we can repeat this process and eventually obtain (for this process will be finite) a P' satisfying (1) in addition to (2) and (3).

Now P' is a p^nth term of a SDP and all the previous terms are in H-ker φ (since all the generators are, by induction hypothesis). Therefore, $\varphi(P')$ is a primitive and thus equals $\sum a_i y_i$, $a_i \in \mathfrak{K}$, $y_i \in \mathfrak{B}$, with coheight y_i = coheight P. If Y_i is the variable corresponding to y_i, let $P_n = P' - \sum a_i Y_i$. Then P_n still satisfies (1), (2), and (3) and, in addition, satisfies (4).

So, for each regular sequence of length n, $n = 0, 1, 2, \ldots, \infty$ in $\mathfrak{F}$, we have a standard sequence $P_0, P_1, \ldots, P_n$ satisfying (1), (2), (3), and (4). The algebra generated by the P_i's will be isomorphic to $\mathfrak{P}_n$. We claim that the coproduct of all such algebras is the H-ker φ. To prove this claim, we must show (1) the P_i are algebraically independent and (2) they generate (as an algebra) H-ker φ.

(1) follows immediately from Lemma 2.15, since the elements of $\mathfrak{F}$ are algebraically independent and are isogeneous.

To prove (2), let $\mathfrak{A}$ be the algebra generated by the P_i. First note that $\mathfrak{A}$ is a Hopf algebra since each $\mathfrak{P}_n$ is. Second, note that if f is a polynomial in the P_i's, coheight $f(P_i)$ in $\mathfrak{A}$ = coheight $f(P_i)$ in $F(\mathfrak{H})$. For by Remark 2.4, coheight $f(P_i)$ in $\mathfrak{A}$, equals the minimum of coheight P_i's in $\mathfrak{A}$ and coheight $f(P_i)$ in $F(\mathfrak{H})$ equals the minimum of the coheight of the variables in $f(P_i)$. But coheight P_i in $\mathfrak{A}$ = coheight P_i in $F(\mathfrak{H})$. Further if $P_i = Q_i + R_i$ with $R_i \in \mathfrak{F}$ and $R_i > Q_i$, then coheight P_i = coheight R_i. But coheight R_i = minimum of the coheight of the variables in R_i, and lastly, since the R_i are algebraically independent and basal, every variable in each R_i appears in $f(R_i)$ and since $R_i > Q_i \; \forall i$, each monomial of $f(R_i)$ is in $f(P_i)$. Thus coheight $f(P_i)$ in $\mathfrak{A} \geqslant$ coheight $f(P_i)$ in $F(\mathfrak{H})$. The opposite inequality is clear.

This fact implies, in particular, that every primitive has the same coheight in $\mathfrak{A}$ and $F(\mathfrak{H})$, or, a fortiori, the same coheight in $\mathfrak{A}$ and H-ker φ.

[1.30] now says that if $\mathfrak{A} \neq H\text{-ker}\,\varphi$, there exists a primitive in H-ker φ which is not in $\mathfrak{A}$.

Let L be one of the smallest such primitives (i.e., its largest monomial is $\succ$ than the largest monomials of other such primitives). By Corollary 3.6, the sum M of the largest monomials in L is in the restricted Lie algebra generated by the variables. By the definition of $\mathfrak{U}$, since M is isogeneous, either $M \in \mathfrak{U}$ or $M = \sum a_i X_i$, $a_i \in \mathfrak{K}$, $X_i \in \mathfrak{T}$. If $M \in \mathfrak{U}$, then by Proposition 3.4 there exists a primitive of the form $M + N$ with $N < M$ and $M + N \in \mathfrak{A}$. ($V(M) = 0$ by 2.13(b) since $V(L) = 0$.) Then $L - (M + N)$ will be a smaller primitive in $(H\text{-ker}\,\varphi) - \mathfrak{U}$. Contradiction.

If $M = \sum a_i X_i$, then since $V(M) = 0$, each X_i is a primitive. Thus $L = M$, and $\varphi(L) \neq 0$, i.e., $L \notin H\text{-ker}\,\varphi$. Q.E.D.

Appendix

Here we show that in the commutative case, $\mathfrak{P}_n$ [Definition 2.6] is isomorphic to $\mathfrak{W}_n$, the Witt Hopf algebra, defined below.

Definition. Let $\mathfrak{W}_n = \mathfrak{K}[S_0, S_1, \ldots, S_n]$ $(0 \leqslant n \leqslant \infty)$ as an algebra. We first define diagonalization over the rationals by letting

$$\begin{aligned} Z_0 &= S_0 \\ Z_1 &= S_1 + (1/p)\, S_0{}^p \\ &\vdots \\ Z_n &= S_n + (1/p)\, S_{n-1}^p + \cdots + (1/p^n)\, S_0^{p^n} \end{aligned}$$

and taking each Z_i to be a primitive. The theory of Witt vectors [6, pp. 49–52] then, states that when we solve for each S_i inductively, the resulting diagonalization will be defined over the integers. This implies that diagonalization can be defined over $\mathfrak{K}$. Finally, let $\epsilon(S_i) = 0$, $\forall i$.

Proposition. $\mathfrak{W}_n \cong \mathfrak{P}_n$ (*commutative*) *as Hopf algebras.*

Proof. We first show that S_i has coheight $n - i$ in $\mathfrak{W}_n$. Assume inductively that S_i has coheight $n - i - 1$ in $\mathfrak{W}_{n-1}$. Then if we show that S_{n-1} has coheight 1 in $\mathfrak{W}_n$, we will have $V(\mathfrak{W}_n) \subset \mathfrak{W}_{n-1}$, and the desired preliminary result will follow.

Now it is straightforward to show that $x \in V(\mathfrak{W}_n)$ is equivalent to

$x \in (\ker F)^{\perp}$, where F is the p-power map on the dual of $\mathfrak{W}_n$. We will show that if $\varphi \in \ker F$, then $\varphi(S_{n-1}) = 0$. Now since $\varphi \in \ker F$, $\varphi^p(S_n) = 0$, i.e.,

$$\underbrace{\varphi \otimes \cdots \otimes \varphi}_{p\text{-times}} (\Delta_{p-1} S_n) = 0.$$

It follows from the definition of the diagonalization, that letting S_i have degree p^i will generate a Hopf algebra grading on $\mathfrak{W}_n$. By our inductive hypothesis, every element x of deg $< p^{n-1}$ has coheight 1, i.e., $\varphi(x) = 0$. Since S_n has degree p^n, if we write $\Delta_{p-1} S_n$ with homogeneous components, the sum of the degrees of the elements of any term of $\Delta_{p-1} S_n$ must be p^n. Therefore, if any term in $\Delta_{p-1} S_n$ contains an element of deg $> p^{n-1}$, it must contain another of deg $< p^{n-1}$ and, therefore, $\varphi \otimes \cdots \otimes \varphi$ applied to this term will be zero. Therefore, the only possible term of $\Delta_{p-1} S_n$ on which $\varphi \otimes \cdots \otimes \varphi$ could not equal zero is $S_{n-1} \otimes \cdots \otimes S_{n-1}$. But

$$\varphi \otimes \cdots \otimes \varphi(\Delta_{p-1} S_n) = 0$$

implies

$$\varphi \otimes \cdots \otimes \varphi(S_{n-1} \otimes \cdots \otimes S_{n-1}) = 0$$

if the coefficient of $S_{n-1} \otimes \cdots \otimes S_{n-1}$ in $\Delta_{p-1} S_n \neq 0$.

To see that this coefficient does not equal zero, diagonalize S_n $(p-1)$-times on the left. The first time we obtain

$$\begin{aligned}\Delta S_n = {} & S_n \otimes 1 + 1 \otimes S_n + d_1 S_{n-1} \otimes S_{n-1}^{p-1} + d_2 S_{n-1}^2 \otimes S_{n-1}^{p-2} + \cdots \\ & + d_{p-1} S_{n-1}^{p-1} \otimes S_{n-1} \\ & + (\text{terms with } S_{n-2} \text{ and lower } S_i\text{'s in them}),\end{aligned}$$

where $d_i = \binom{p}{i}/p$.

Certainly, the only term here that could yield, when diagonalized on the left, a

$$\underbrace{S_{n-1} \otimes \cdots \otimes S_{n-1}}_{p\text{-times}}$$

is $d_{p-1} S_{n-1}^{p-1} \otimes S_{n-1}$. Now $\Delta S_{n-1} = S_{n-1} \otimes 1 + 1 \otimes S_{n-1} +$ (terms with lower S_i's in them), so

$$\begin{aligned}\Delta S_{n-1}^{p-1} = {} & S_{n-1}^{p-1} \otimes 1 + \binom{p-1}{1} S_{n-1}^{p-2} + \cdots + 1 \otimes S_{n-1}^{p-1} \\ & + (\text{terms with smaller } S_i\text{'s in term}).\end{aligned}$$

Again, the only candidate is $S_{n-1}^{p-2} \otimes S_{n-1}$. Continuing we find that

$$\Delta_{p-2} S_{n-1}^{p-1} = (p-1)!\, S_{n-1} \otimes \cdots \otimes S_{n-1} + (\text{other terms}).$$

Therefore, the coefficient of $S_{n-1} \otimes \cdots \otimes S_{n-1}$ in $\Delta_{p-1}S_n$ is $((p-1)!\, d_{p-1} = (p-1)! \not\equiv 0 \bmod p$. Thus, we conclude that $\varphi(S_{n-1}) = 0$, i.e., S_{n-1} has coheight 1.

Note that we now have that $V(S_i) = S_{i-1}$, $i \geqslant 1$, since S_{i-1} has coheight 1 in $\mathfrak{W}_i$, but not in $\mathfrak{W}_{i-1}$, and $V^{-1}(S_{i-1})$ has degree p^i [1.20]. Thus $S_0, S_1, \ldots, S_n$ forms a regular sequence. Now apply Corollary 2.11, with $\mathfrak{F}_i = \mathfrak{W}_{i-1}$. We obtain a standard sequence whose ith generator is of the form $S_i + T_i$ with $T_i \in \mathfrak{W}_{i-1}$. Clearly the map $\mathfrak{P}_n \to \mathfrak{W}_n$ generated by $Y_i \to S_i + T_i$ will be a Hopf algebra isomorphism.

Remark. The above proposition is true over arbitrary fields of char p. Just construct the isomorphism over the prime field and extend everything by scalars.

BIBLIOGRAPHY

1. C. W. CURTIS, Review of [10], *Math. Rev.* **17** (1957), 1050.
2. B. DITTERS, Curves in formal groups, unpublished.
3. R. HEYNEMAN AND M. E. SWEEDLER, Affine Hopf algebras II, *J. Algebra* **16** (1970), 271–297.
4. N. JACOBSON, "Lie Algebras," Interscience Publishers, New York, 1962.
5. K. NEWMAN, Sequences of divided powers in irreducible, cocommutative Hopf algebras, *Trans. Amer. Math. Soc.* **163** (1972), 25–34.
6. J. P. SERRE, "Corps Locaux," Hermann, Paris, 1962.
6′. C. SCHOELLER, Étude de la catégorie des algèbres de Hopf commutatives connexes sur un corps, *Manuscripta Math.* **3** (1970), 133–155.
7. H. STOLBERG, Ph.D. Thesis, Cornell University, Ithaca, NY, 1969.
8. M. E. SWEEDLER, "Hopf Algebras," W.A. Benjamin, New York, 1969.
9. M. E. SWEEDLER, Hopf algebras with one grouplike, *Trans. Amer. Math. Soc.* **127** (1967), 515–526.
10. E. WITT, Die Unterringe der frein Lieschem Ringe, *Math. Z.* **64** (1956), 195–216.